UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/955,902	09/18/2001	Mihailo M. Stojancic	50325-0550	9907

29989 7590 01/06/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/955,902	STOJANCIC ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3-08-2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 09/18/2001

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> **The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.**

2. Claims 15 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 15 and 16 are indefinite because, in conjunction with the independent claim 1, the claim language "intermediate result" is based on the modular operation (Claim 1 Line 11 – 12) where modular operation is again based on the intermediate result (Claim 15 Line 1 – 3 and Claim 16 Line 1 – 4) and thereby constitutes an indefinite feedback function because it is not clearly and uniquely pointed out what constitutes the "intermediate result" as any of other parameters does in the claim limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 – 16 and 27 – 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Langston (Patent Number: US 2003/0031316 A1), hereinafter referred to as Langston, in view of Dror (Patent Number: US 2002/0039418 A1), hereinafter referred to as Dror.

As per claim 1, Langston teaches a method for encryption and decryption of electronic messages based on an encryption protocol, the method comprising the computer-implemented steps of:

receiving a first electronic message that is encrypted according to the encryption protocol (Langston: see for example, Paragraph [0050] Line 15 – 16 and Paragraph [0010] Line 6: The partial product (or intermediate result) of improved modular cryptography system using RSA ciphering key / protocol is interpreted as the first electronic message of RSA encryption protocol).

generating at least one part of a second electronic message (Langston: see for example, Claim 9 and Paragraph [0048] Line 8 – 9: the final result for the

modulo exponentiation is considered as the second electronic message) based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and wherein the step of generating the second electronic message includes the computer-implemented steps of:

generating a first constant based on the modulus (Langston: see for example, Claim 11 (ii));

Langston teaches determining an intermediate result (Langston: see for example, Claim 5).

Langston does not disclose expressly determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant.

Dror teaches determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant (Dror: see for example, Paragrah [0312] – [0326]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Dror within the system of Langston because Dror teaches using Montgomery reduction with partial products to perform an efficient multiplication operations so that shorter operands, registers, and hardware multipliers are needed (Dror: see for example, Paragraph [0332]).

Langston as modified further teaches:

determining and storing in memory a final result that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand (Langston: see for example, Paragraph [0048] Line 8 – 9).

As per claims 2, 3 and 4, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the encryption protocol is the Rivest-Shamir-Adleman public key protocol or Diffie-Hellman key agreement protocol or digital signature algorithm protocol (Langston: see for example, [0010] Line 6: Diffie-Hellman key agreement protocol and digital signature algorithm protocol use the equivalent or similar cryptography approach to the -Shamir-Adleman public key protocol).

As per claims 5 and 6, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the step of generating the first constant (R) based on the modulus (M) includes the computer-implemented steps of: selecting a second constant (W) such that W >= 4M; and determining the first constant (R) according to the expression $R = W^2 \pmod{M}$ (Langston: see for example, claim 15: Montgomery constant as taught by Langston corresponds to W^2, where $W = r^{(n+8)}$).

As per claim 7, Langston as modified teaches the claimed invention as

described above (see claim 6). Langston as modified further teaches the second constant (W) is not a power of two (Langston: see for example, claim 15: r can be any number).

As per claim 8, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the first operand is a first 1024-bit operand and the second operand is a second 1024-bit operand (Langston: see for example, Paragraph [0010] Line 6).

As per claims 9 and 10, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the modular operation is a modular multiplication that is based on at least the first operand (X), the first constant (R), a second constant (W), the modules (M), and a negative multiplicative inverse of the modules (M'), and wherein the intermediate result (S) is determined based on the following expressions: Z=XR; U = ZM'(mod(W)); and S = (Z + UM)/W (Dror: see for example, Paragraph [0312] – [0326]).

As per claims 11 and 12, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the modular operation is a modular multiplication that is based on at least the second operand (Y), a second constant (W), the modulus (M), a negative

multiplicative inverse of the modulus (M'), and the intermediate result (S), and wherein the final result (F) is determined based on the following expressions Z = YS; U = ZM'(mod(VV)); and F = (Z + UM)/W (Dror: see for example, Paragraph [0312] – [0326]).

As per claims 13 and 14, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the modular operation is a modular exponentiation that is based on at least the first operand (X), the first constant (R), a second constant (W), the modules (M), and a negative multiplicative inverse of the modules (M7, and wherein the intermediate result (S) is determined based on the following expressions: Z = XR; U = ZM'(mod(W)); and S=(Z+UM)IW (Dror: see for example, Paragraph [0312] – [0326]: modular exponentiation is actually inherent from the modular multiplication – e.g. $X^2 = X * X$) & (Langston: see for example, Claim 23: modular exponentiation as taught by Langston comprising "iteratively" computing running "partial product" i.e. intermediate result).

As per claims 15 and 16, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified further teaches the modular operation is a modular exponentiation that is based on at least the second operand, a second constant, the modules, a negative multiplicative inverse of the modules, and the intermediate result, wherein the second operand includes

a plurality of digits, and wherein the final result is determined by the computer implemented steps of (Dror: see for example, Paragraph [0312] – [0326]: modular exponentiation is actually inherent from the modular multiplication – e.g. $X^2 = X * X$) & (Langston: see for example, Claim 23: modular exponentiation as taught by Langston comprising "iteratively" computing running "partial product" i.e. intermediate result).:

specifying a previous final result as having a value of one and a previous intermediate result as the intermediate result (Langston: see for example, Paragraph [0050] Line 15 – 16 & Claim 5);

for each digit of the plurality of digits included in the second operand, performing the computer-implemented steps of: and when each digit of the plurality of digits has the value of one, then performing the computer-implemented steps of:

determining an updated final result based on the previous final result and the previous intermediate result (Langston: see for example, Claim 23: modular exponentiation as taught by Langsto comprising "iteratively" computing running "partial product" i.e. intermediate result);

determining a modular reduction of the updated final result based on the updated final result, the negative multiplicative inverse of the modules, and the second constant (Langston: see for example, Claim 9 and Paragraph [0048] Line 8 – 9) and (Dror: see for example, Paragrah [0326]);

determining a revised updated final result based on the updated final result,

the modular reduction of the final result, the modulus, and the second constant (Langston: see for example, Claim 23) and (Dror: see for example, Paragrah [0312] – [0326]);

if all digits of the plurality of digits have not been evaluated, specifying the revised updated final result as the previous final result (Langston: see for example, Claim 23 & Claim 24 and 39); and

if all digits of the plurality of digits have been evaluated, specifying. the revised updated final result as the final result (Langston: see for example, Claim 23: modular exponentiation as taught by Langsto comprising "iteratively" computing running "partial product" i.e. intermediate result);

determining an updated intermediate result based on the previous intermediate result (Langston: see for example, Claim 23: modular exponentiation as taught by Langsto comprising "iteratively" computing running "partial product" i.e. intermediate result);

determining a modular reduction of the updated intermediate result based on the updated intermediate result, the negative multiplicative inverse of the modulus, and the second constant (Langston: see for example, Claim 23) and (Dror: see for example, Paragrah [0312] – [0326]);

determining a revised updated intermediate result based on the updated intermediate result, the modular reduction of the updated intermediate result, the modulus, and the first constant (Langston: see for example, Claim 23) and (Dror: see for example, Paragrah [0312] – [0326]); and

specifying the revised updated intermediate result as the previous intermediate result (Dror: see for example, Paragraph [0312] – [0326]: modular exponentiation is actually inherent from the modular multiplication – e.g. $X^2 = X * X$) & (Langston: see for example, Claim 23: modular exponentiation as taught by Langston comprising "iteratively" computing running "partial product" i.e. intermediate result as the revised updated intermediate result).

As per claim 27 – 33, Langston as modified teaches the claimed invention as described above (see claim 1, 27, 29, 31 and 33 respectively). Langston as modified further teaches modular operation is a modular multiplication and the step of generating the second electronic message further includes the computer-implemented step of: while determining the intermediate result and. determining the final result, storing results of intermediate computations in a first register file and a second register file (Langston: see for example, Claim 24 and 39: The number of registers and the bit size used are considered as the result of design choice and implementation details).

As per claim 34, 35 and 36, claims 34, 35 and 36 do not further teach over claim 1, 10 and 12. Therefore, see same rationale addressed above in rejecting claim 1, 10 and 12.

4. Claims 17 – 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Langston (Patent Number: US 2003/0031316 A1), hereinafter referred to as Langston, in view of Dror (Patent Number: US 2002/0039418 A1), hereinafter referred to as Dror, and in view of Posch (Modulo Reduction in Residue Number Systems: IEEE Transaction on Parallel Distributed Systems Vol.6, No.5 May 1995), hereinafter referred to as Posch.

As per claim 17, Langston as modified teaches the claimed invention as described above (see claim 1). Langston as modified does not disclose the computer implemented steps of: generating a plurality of residual number system (RNS) representations, wherein the plurality of RNS representations includes at least one RNS representation for each of the first operand, the modulus, and the first constant; wherein the step of determining the intermediate result includes the computer-implemented step generating the intermediate result based on Montgomery's method for the modular operation and the plurality of RNS representations; and wherein the step of determining the final result includes the computer-implemented step of generating the final result based on Montgomery's method for the modular operation and the plurality of RNS representations.

Posch teaches the computer-implemented steps of: generating a plurality of residual number system (RNS) representations in combination with Montgomery's method (Posch: see for example, 1st and 2nd Paragraphs of Introduction section).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Posch within the system of Langston as modified because Posch teaches employing residual number system (RNS) with the Montgomery reduction method to yield powerful / efficient performance (Posch: see for example, Paragraph [0332]).

Therefore Langston as modified teaches the plurality of RNS representations includes at least one RNS representation for each of the first operand, the modulus, and the first constant; wherein the step of determining the intermediate result includes the computer-implemented step generating the intermediate result based on Montgomery's method for the modular operation and the plurality of RNS representations; and wherein the step of determining the final result includes the computer-implemented step of generating the final result based on Montgomery's method for the modular operation and the plurality of RNS representations (Langston: see for example, Paragraph [0050] Line 15 – 20, Claim 5 – 10) & (Dror: see for example, Paragraph [0312] – [0326]) & (Posch: see for example, 1st and 2nd Paragraphs).

As per claim 18, 19 and 20, Langston as modified teaches the claimed invention as described above (see claim 17, 18 and 19 respectively). Langston as modified further teaches the plurality of RNS representations includes a first set of RNS representations in a first RNS base and a second set of RNS representations in a second RNS base (Posch: see for example, Page 452 Right Column item (3)).

As per claim 21 – 26, Langston as modified teaches the claimed invention as described above (see claim 19 and 22 respectively). Langston as modified further teaches the step of converting is performed in eight clock cycles (Posch: see for example, Page 453 Right Column Last 2nd Paragraph: The number of clock cycles, the number of residues and its associated bit-size used are considered as the result of design choice and implementation details).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AU2131
12/29/04